CHAPTER 2

COMMAND SECURITY MANAGEMENT

2-1 BASIC POLICY

Commanding officers are responsible for compliance with and implementation of the DON Information and Personnel Security Program within their command. The effectiveness of the command's security program depends on the importance the commanding officer gives it.

2-2 COMMANDING OFFICER

1. An effective security program relies on a team of professionals working together to fulfill the commanding officer's responsibilities.

2. Command security management responsibilities include:

a. Designate a security manager.

b. Designate a Top Secret control officer (TSCO) if the command handles Top Secret information.

c. Designate an information systems security manager (ISSM) if the command processes data in an automated system.

d. Designate a security officer to manage facilities security.

e. Designate a Special Security Officer (SSO) to administer the command SCI security program.

f. Issue a written command security instruction. See appendix C and exhibit 2A of reference (d).

g. Establish an industrial security program when the command engages in classified procurement or when cleared contractors operate within areas under the commanding officer's control.

h. Ensure that the security manager and other command security professionals are appropriately trained, that all personnel receive required security education and that the command has a robust security awareness program.

i. Prepare an emergency plan for the protection of classified material.

j. Ensure that command security inspections, program reviews, and assist visits to subordinate commands are conducted, as determined necessary.

k. Ensure that the performance rating systems of all DON military and civilian personnel, whose duties significantly involve the creation, handling, or management of national security information (NSI), include a security element on which to be evaluated.

2-3 SECURITY MANAGER

1. Every command in the Navy and Marine Corps eligible to receive classified information is required to designate a security manager **in writing**.

2. The security manager will be afforded direct access to the commanding officer to ensure effective management of the command's security program.

3. The command security manager may be assigned full-time, part-time or as a collateral duty and must be an officer or a civilian employee, GS-11 or above, with sufficient authority and staff to manage the program for the command. The security manager must be a U.S. citizen and have been the subject of a favorably adjudicated SSBI completed within the previous 5 years.

4. The command security manager must be designated by name and identified to all members of the command on organization charts, telephone listings, rosters, etc. OPNAVINST 3120.32C, Standard Organization and Regulations of the U.S. Navy (NOTAL), recommends the security manager report to the commanding officer for functional security matters and to the executive officer for administrative matters.

5. Commanding officers are strongly encouraged to obtain formal training for their security managers. The Navy Security Managers Course offered by the Naval Criminal Investigative Service (NCIS) Mobile Training Team (MTT), is highly recommended.

2-4 DUTIES OF THE SECURITY MANAGER

1. The security manager is the principal advisor on information and personnel security in the command except issues specific to SCI and other special access program information and is responsible to the commanding officer for the management of the program. The duties described here and in chapter 2 of reference (d) may be assigned to a number of personnel and may even be

assigned to individuals senior to the security manager. However, the security manager remains ultimately responsible for all program requirements. The security manager must be cognizant of the command security functions and ensure the security program is coordinated and inclusive of all requirements. The security manager must ensure that those in the command who have security duties are kept abreast of changes in policies and procedures, and must provide assistance in solving security problems. The job may involve direct supervision, oversight, coordination, or a combination thereof. The security manager is the key in developing and administering the command's Information and Personnel Security Program.

2. The below listed duties and those provided in chapter 2 of reference (d), apply to every security manager:

a. Serves as the commanding officer's advisor and direct representative in matters pertaining to the security of classified information held at the command.

b. Serves as the commanding officer's advisor and direct representative in matters regarding the eligibility of personnel to access classified information and to be assigned to sensitive duties.

c. Develops written command information and personnel security procedures, including an emergency plan which integrates emergency destruction bills where required.

d. Formulates and coordinates the command's security awareness and education program.

e. Ensures security control of visits to and from the command when the visitor requires, and is authorized, access to classified information.

f. Ensures that all personnel who will handle classified information or will be assigned to sensitive duties are appropriately cleared through coordination with the DON CAF and that requests for personnel security investigations are properly prepared, submitted and monitored.

g. Ensures that access to classified information is limited to those who are eligible and have the need to know.

h. Ensures that personnel security investigations, clearances and accesses are properly recorded.

i. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties.

j. Maintains liaison with the command SSO concerning information and personnel security policies and procedures.

k. Coordinates with the command information systems security manager on matters of common concern.

l. Ensures that all personnel who have had access to classified information who are separating or retiring have completed a Security Termination Statement. The original statement is filed in the individual's field service record or official personnel file and a copy in the command files.

m. Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information.

2-5 TOP SECRET CONTROL OFFICER (TSCO)

Commands that handle Top Secret material will designate a TSCO **in writing**. The TSCO must be an officer, senior non-commissioned officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U.S. citizen and have been the subject of a SSBI completed within the previous 5 years. Duties of a TSCO are listed in chapter 2 of reference (d).

2-6 OTHER SECURITY ASSISTANTS

1. **Assistant Security Manager**. Persons designated as assistant security managers must be U.S. citizens, and either officers, enlisted persons E-6 or above, or civilians GS-6 or above. The designation must be **in writing**. Assistant security managers must have an SSBI if they are designated to issue interim security clearances; otherwise, the investigative and clearance requirements will be determined by the level of access to classified information required.

2. **Security Assistant.** Civilian and military member employees performing administrative functions under the direction of the security manager may be assigned without regard to rate or grade as long as they have the clearance needed for the access required to perform their assigned duties and taskings.

3. **Top Secret Control Assistant (TSCA)**. Individuals may be assigned to assist the TSCO as needed. The designation will be

in writing. A person designated as a TSCA must be a U.S. citizen and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. An established Top Secret security clearance eligibility is required. Top Secret couriers are not considered to be Top Secret control assistants. Duties of a TSCA are listed in chapter 2 of reference (d).

2-7 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

Commands that award classified contracts to industry will appoint, **in writing**, one or more qualified security specialists as the Contracting Officer's Representative (COR). The COR is responsible to the security manager for coordinating with program managers and technical and procurement officials. The COR will ensure that the industrial security functions are accomplished when classified information is provided to industry for performance on a classified contract.

2-8 INFORMATION SYSTEMS SECURITY MANAGER (ISSM)

1. Each command involved in processing data in an automated system, including access to local area networks and/or INTRANET/INTERNET, must designate a civilian or military member as an ISSM.

2. The ISSM is responsible to the commanding officer who develops, maintains, and directs the implementation of the INFOSEC program within the activity. The ISSM advises the commanding officer on all INFOSEC matters, including identifying the need for additional INFOSEC staff. The ISSM serves as the command's point of contact for all INFOSEC matters and implements the command's INFOSEC program.

2-9 SPECIAL SECURITY OFFICER (SSO)

1. Commands in the DON accredited for and authorized to receive, process and store SCI will designate an SSO. The SSO is the principal advisor on the SCI security program in the command and is responsible to the commanding officer for the management and administration of the program. SCI security program responsibilities are detailed in reference (c). The SSO will be afforded direct access to the commanding officer to ensure effective management of the command's SCI security program. The SSO will be responsible for the operation of the Sensitive Compartmented Information Facility (SCIF) and the security control and use of the SCIF. All SCI matters are referred to the SSO.

2. The SSO and the subordinate SSO will be appointed **in writing** and each will be a U.S. citizen and either a commissioned officer or a civilian employee GS-9 or above, and must meet Director, Central Intelligence Directive (DCID) 1/14, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)" (NOTAL) standards. The same grade limitations apply to assistant SSOs. The security manager cannot function as the SSO unless authorized by the Director, ONI or COMNAVSECGRU. The SSO will be responsible for the operation of the SCIF and the security control and use of the SCIF. All SCI matters are referred to the SSO.

3. Although the SSO administers the SCI program independent of the security manager, the security manager must account for all clearance and access determinations made on members of the command. There is great need for cooperation and coordination between the SSO and security manager, especially for personnel security matters. For individuals who are SCI eligible, the security manager and the SSO must keep one another advised of any changes in status regarding clearance and access and of information developed that may affect eligibility. The security manager and SSO must also advise each other of changes in SCI and command security program policies and procedures as they may impact on the overall command security posture.

2-10 INSPECTIONS, ASSIST VISITS, AND REVIEWS

1. Commanding officers are responsible for evaluating the security posture of their subordinate commands.

2. Senior commanders may, as determined necessary, conduct inspections, assist visits, and reviews to examine overall security posture of subordinate commands. Unless otherwise required, it is not necessary to conduct separate inspections for security. They may be conducted during other scheduled inspections and results identified as such.

3. A command personnel security program self-inspection guide is provided as appendix D.

4. Refer to exhibit 2C of reference (d) for the ISP self-inspection guide.

2-11 SECURITY SERVICING AGREEMENTS

1. Commands may perform specified security functions for other commands via security servicing agreements. Such agreements may

be appropriate in situations where security, economy, and efficiency are considerations, including;

a. A command provides security services for another command, or the command provides services for a tenant activity;

b. A command is located on the premises of another government entity and the host command negotiates an agreement for the host to perform security functions;

c. A senior in the chain of command performs or delegates certain security functions of one or more subordinate commands;

d. A command with particular capability for performing a security function agrees to perform the function for another;

e. A command is established expressly to provide centralized service (for example, Personnel Support Activity or Human Resources Office); or

f. When either a cleared contractor facility or a long term visitor group is physically located on a Navy or Marine Corps installation.

2. A security servicing agreement will be specific and must clearly define where the security responsibilities of each participant begin and end. The agreement will include requirements for advising commanding officers of any matters which may directly affect the security posture of the command. Append security servicing agreements to the command security instruction.

2-12 STANDARD PROGRAM REQUIREMENTS

Each command which handles classified information is required to prepare and keep current a written command security instruction, specifying how security procedures and requirements will be accomplished in the command. Appendix C and exhibit 2A of reference (d) pertain.

2-13 PLANNING FOR EMERGENCIES

Commands will establish a plan for the protection and removal of classified NSI under its control during emergencies. Depending upon the location of the command, the plan may direct destruction of classified NSI in an emergency. The plan should be made part of the overall disaster preparedness plan of the command security program instruction. See reference (d), exhibit 2B.